UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/885,427	06/19/2001	Peter A.J. van der Made	81924.0002	4888

7590 04/03/2006

W SCOTT PETTY
KING & SPALDING
191 PEACHTREE STREET 45TH FLOOR
ATLANTA, GA 30303-1763

EXAMINER	
GUILL, RUSSELL L	
ART UNIT	**PAPER NUMBER**
2123	

DATE MAILED: 04/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/885,427	MADE, PETER A.J. VAN DER	
	Examiner	Art Unit	
	Russell L. Guill	2123	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 January 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *11, 13 - 14, 17 - 23, 26 - 30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *11, 13 - 14, 17 - 23, 26 - 30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 September 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *7/11/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to an Amendment filed January 20, 2006. Claims 1 - 10, 12, 15 - 16 and 24 - 25 have been cancelled. Claims 11, 13 - 14, 17 - 23, and 26 - 30 are pending. Claims 11, 13 - 14, 17 - 23, and 26 - 30 have been examined. Claims 11, 13 - 14, 17 - 23, and 26 - 30 have been rejected under 35 U.S.C. § 112.

Response to Remarks

2. As requested by the Applicant, the Examiner has reviewed and approved the interview record, and attached it to this Office Action.

3. Regarding claim 27 rejected under 35 U.S.C. § 112:

   a. Applicant's amendment to the claim overcomes the rejection, and accordingly, the rejection is withdrawn.

4. Regarding claims 11 - 16, 18 - 25 and 27 - 30 rejected under 35 U.S.C. § 103:

   a. Applicant's amendments to the claims and arguments (see pages 9 - 19 of the arguments) have been fully considered, and are persuasive. However, Applicant's amendments to the claims have resulted in 35 U.S.C. 112 rejections.

Information Disclosure Statement

5. The Examiner would like to note that several documents listed on the Information Disclosure Statement (IDS), filed on July 11, 2005, do not appear to have been included with the IDS. The missing documents are noted on the IDS by a line through the entry.

Claim Objections

6. Claim 22 is objected to because of the following informalities: The claim recites "one or more programs." The antecedent appears to refer to program modules. Reference to

the previous limitation should remain consistent to avoid any possible confusion or antecedent issues. Appropriate correction is required.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

a. **Claims 11, 13 - 14, 17 - 23, and 26 - 30** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

i. Regarding **claims 11, 20 and 29**, the claims recite, "executing DOS and Windows type target programs." The term "type" makes the claim vague and indefinite. It is not possible to determine the metes and bounds of the claims. Further, the term "Windows" is a trademark. The claim scope is uncertain since the trademark or trade name cannot be used properly to identify any particular material or product. For the purpose of claim examination, the phrase, "executing DOS and Windows type target programs" is interpreted as "executing DOS target programs." Correction or amendment is required.

ii. Regarding **claim 29**, the claim recites, "the file format" and "the computer system." The terms have insufficient antecedent basis. For the purpose of claim examination, the phrase, "the file format" is interpreted as "a file format." For the purpose of claim examination, the phrase, "the computer system" is interpreted as "a computer system." Correction or amendment is required.

iii. **Claims 13 - 14, 17 - 19, 21 - 23, 26 - 28 and 30** are rejected based on their dependency on their respective intermediate and parent claims which are rejected under 35 U.S.C. 112.

Allowable Subject Matter

8. **Claims 11, 20 and 29** would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action.

9. **Claims 13 - 14, 17 - 19, 21 - 23, 26 - 28 and 30** would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

10. The following is a statement of Examiner's reasons that the Applicant's invention defines over the prior art of record:

a. While Le Charlier ("Dynamic Detection and Classification of Computer Viruses Using General Behavior Patterns", 1995) and Custer ("Inside Windows NT", 1993) and Chi (U.S. Patent No. 5,978,917) teach a computer implemented method and a system for identifying malicious code in a target program, including automatically configuring the virtual machine to execute the target program, in one of three modes of operation based on the file format and the control fields within the header of the file, a first mode of operation comprising a real mode for executing programs comprising instructions based on DOS, a second mode of operation for executing target programs comprising a high level programming language, and a third mode of operation comprising a protected

mode for executing target programs comprising thirty-two bit code; simulating values of the computer system with the one or more layered operating system shells of the virtual machine; setting behavior flags in order to track behavior of the target program in response to the simulated values, during execution of the target program by the virtual machine; storing a sequence in which the behavior flags are set in the register by the target program during execution of the target program by the virtual machine; passing behavior flag data and sequence flag data from the virtual machine to the computer system for evaluation after execution of the target program by the virtual machine; and evaluating the behavior flag data and sequence flag data with the computer system to determine if the target program contains malicious code, none of these references taken either alone or in combination with the prior art of record teach a computer implemented method and a system for identifying malicious code in a target program running in a virtual machine of a computer system specifically including:

i. **Claims 11, 20 and 29**: "automatically configuring a memory map of the virtual machine by assigning areas of the memory map to receive predetermined types of data from the target program based on the file format in order to execute the target program," "constructing the virtual machine from one or more layered operating system shells that correspond with the memory map so that the virtual machine is capable of executing DOS and Windows type target programs," "setting and resetting behavior flags in a register in order to track behavior of the target program in response to the simulated values, during execution of the target program by the virtual machine," and "storing a sequence in which the behavior flags are set and reset in the register by the target program during execution

of the target program by the virtual machine," in combination with the remaining elements and features of the claimed invention.

It is for these reasons that the Applicant's invention defines over the prior art of record.

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Russell L. Guill whose telephone number is 571-272-7955. The examiner can normally be reached on Monday - Friday 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Paul Rodriguez can be reached on 571-272-3753. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Any inquiry of a general nature or relating to the status of this application should be directed to the TC2100 Group Receptionist: 571-272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Russ Guill
Examiner
Art Unit 2123

RG

Paul L. Rodriguez
Primary Examiner
Art Unit ~~2125~~ 2123
3/30/02